Théorème de l'élément primitif

Référence : [FG97].

Théorème 0.1 (de l'élément primitif) *Soit $\mathbb{K} = \mathbb{F}_q \subset L = \mathbb{F}_{q^n}$ où q désigne une puissance d'un nombre premier. Alors il existe $\alpha \in L$ tel que :*

$$L = \mathbb{K}(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)}, P, Q \neq 0 \in \mathbb{K}[X] \right\}$$

Démonstration Montrons que $\mathbb{F}_{q^n}^*$ est cyclique car alors si α est un générateur de $\mathbb{F}_{q^n}^*$, il est clair que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$.
Pour démonter cela nous allons utiliser deux lemmes.

Lemme 0.1 *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

Démonstration Soit $\mathbb{K}$ un corps et G un sous-groupe fini de $(\mathbb{K}^*, \times)$. Soit $n = |G|$. Pour d divisant n, on note :

$$A_d = \{x \in G; \quad x \text{ d'ordre } d\}$$

On a :

$$G = \bigcup_{d|n} A_d$$

Soit $d|n$ et supposons que $A_d \neq \emptyset$. Soit $x \in A_d$ et H_d le groupe cyclique d'ordre d engendré par x. Alors on a : $|A_d| \geq \phi(d)$ car tous les générateurs de H_d sont dans A_d.
D'autre part, les éléments de H_d sont racines du polynôme $X^d - 1$, polynôme qui a au plus d racines et H_d a d éléments. Donc H_d est exactement l'ensemble des racines de ce polynôme, ie $H_d \simeq \mathbb{Z}/d\mathbb{Z}$, ie le nombre d'éléments d'ordre d est $\phi(d)$ puisque $\mathbb{Z}/d\mathbb{Z}$ est cyclique.
Ainsi si $y \in A_d$, le groupe engendré par y est aussi H_d, donc $A_d \subset H_d \simeq \mathbb{Z}/d\mathbb{Z}$ et donc $|A_d| = \phi(d)$.
Posons :

$$\epsilon_d = \begin{cases} 1 & \text{si } A_d \neq \emptyset\,; \\ 0 & \text{si } A_d = \emptyset. \end{cases}$$

On a donc :

$$n = \sum_{d|n} \epsilon_d \phi(d)$$

puisque les A_d forment une partition de G.
De plus, on a également :

$$n = \sum_{d|n} \phi(d)$$

Donc, comme pour tout diviseur d de n, on a $\phi(d) \neq 0$, tous les ϵ_d valent 1. En particulier $\epsilon_n = 1$, ie $A_n \neq \emptyset$, ie il existe un élément d'ordre n dans G. Or le sous-groupe engendré par cet élément donne une sous-groupe de G de cardinal $n = |G|$, donc ce sous-groupe, qui est cyclique, est G.

Lemme 0.2

$$n = \sum_{d|n} \phi(d)$$

Démonstration
Étape 1 Montrons que tout sous-groupe d'un groupe cyclique est cyclique.
Soit G un groupe cyclique engendré par x. Soit H un sous-groupe de G non réduit à $\{e\}$. Soit :

$$d = \inf\{k \in \mathbb{N}^*; x^k \in H \setminus \{e\}\}$$

Soit $x^k \in H$, alors il existe $(q, r) \in \mathbb{N}^2$ tels que :

$$k = qd + r \quad \text{avec} \quad 0 \leq r < d$$

On a donc :

$$x^k = \left(x^d\right)^q x^r$$

et comme $x^k \in H$ et $x^d \in H$ et H est un sous-groupe alors $x^r \in H$, ie $r = 0$ par définition de d.
Ainsi x^d engendre H, qui est donc bien cyclique.

Étape 2 Soient $(d, n) \in \mathbb{N}^2$ où d divise n. Montrons qu'il existe un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
Soit :

$$H = \{x \in \mathbb{Z}/n\mathbb{Z}; dx = 0\}$$

H est un sous-groupe qui contient tout sous-groupe d'ordre d. En particulier $\{\overline{0}, \overline{k}, \ldots, \overline{(d-1)k}\}$ où $k = \dfrac{n}{d}$. Donc $|H| \geq d$.
D'autre part, H est cyclique d'après l'étape 1 et tout générateur a un ordre divisant d, donc $|H||d$, en particulier $|H| \leq d$.
Par conséquent $|H| = d$ et tout sous-groupe d'ordre d est égal à H.

Étape 3 Montrons la formule voulue.
Tout élément de $\mathbb{Z}/n\mathbb{Z}$ a un ordre divisant n d'après le théorème de Lagrange et donc :

$$G = \bigcup_{d|n} A_d$$

où A_d est l'ensemble des éléments d'ordre d.
Les éléments de A_d sont les générateurs de l'unique sous-groupe d'ordre d isomorphe à $\mathbb{Z}/d\mathbb{Z}$; il y en a $\phi(d)$. D'où le résultat.

Références

[FG97] Serge Francinou and Hervé Gianella. *Exercices de mathématiques pour l'agrégation : algèbre 1*. Masson, 1997.